Computing general error locator polynomial of 3-error-correcting BCH codes via syndrome varieties using minimal polynomial

Muhammad Zaki Almuzakki[a,b] and Katsuyoshi Ohara[c]

[a]Graduate School of Natural Science and Technology, Kanazawa University, Japan
[b]Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Indonesia, E-mail: muhammad.almuzakki@gmail.com
[c]Faculty of Mathematics and Physics, Kanazawa University, Japan, E-mail: ohara@air.s.kanazawa-u.ac.jp

Abstract. *BCH codes are subclass of cyclic codes with strong properties and have been known for years. In 1994, Chen, Reed, Helleseth, and Truong proposed a decoding procedure for t-error-correcting codes via CRHT syndrome variety using computation of lexicographical Gröbner bases of the ideal. In 2005, Orsini and Sala added polynomial $\chi_{l,\tilde{l}}$, $1 \leq l < \tilde{l} \leq t$, to a system of algebraic equations I to make sure that the position of any two errors are distinct or at least one of them is zero. In 2014, Takuya Fushisato proposed a modified system J to solve 2-error-correcting BCH codes problem. Here the polynomial $\tau_j \in J$ is a divisor of σ_j and contain all possible syndromes of type $0, \alpha^{i_1}, \alpha^{i_1} + \alpha^{i_2} \in \mathbb{F}_{q^m}$ as roots. Generally, τ_j may be regarded as the minimal polynomial of the roots. In this paper, Fushisato's system is generalized into K in which $\Omega_j \in K$ contains all possible roots of t-error-correcting BCH codes in the set $Sol \subseteq \mathbb{F}_{q^m}$. Using the system of polynomials K, the general error locator polynomials of 3-error-correcting codes could be computed and the computation time of some codes were reduced.*

Keywords: BCH codes, t-error-correcting codes, CRHT syndrome variety

1 Introduction

Communication is one of essential components of human beings. The main purpose of a communication system is to deliver any messages effectively from sender to receiver. In a communication system, there are many possibilities that there will be errors due to communication channel. To overcome these problems, researchers develop a field of study named *coding theory*. In general, coding theory deals with the construction of strong codes with good encoding and decoding procedures. Some codes with strong properties are called BCH codes. BCH codes are subclass of cyclic codes in which many algebraic tools can be applied.

Let $\mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^m}$ be a primitive nth root of unity such that

$$\prod_{i=0}^{n-1}(x - \alpha^i) = x^n - 1.$$

A BCH code C can be seen as $\mathbb{F}_q$-kernel of parity-check matrix

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_r} & \alpha^{2i_r} & \dots & \alpha^{(n-1)i_r} \end{pmatrix}.$$

Assume that there are errors in the transmission. The errors are collected in an error vector

$$\vec{e} = (e_0 \dots e_{n-1}) = (\underbrace{0\dots 0}_{k_1-1} \underset{k_1}{\underset{\uparrow}{a_1}} 0 \dots 0 \underset{k_l}{\underset{\uparrow}{a_l}} 0 \dots 0 \underset{k_t}{\underset{\uparrow}{a_t}} \underbrace{0\dots 0}_{n-k_t-1})$$

where t is the maximum number of errors, $k_1, \dots, k_t$ denote the error location and $a_1, \dots, a_t$ denote the error value. Then the syndrome vector can be computed by multiplying parity-check matrix H with the transpose of error vector $\vec{e}^T$. That is, $\vec{s}^T = H\vec{e}^T$. Every entry s_j of $\vec{s}^T$ can be written in following equation,

$$\sum_{l=1}^{t} a_l (\alpha^{i_j})^{k_l} - s_j = 0, \ 1 \le j \le r \tag{1}$$

To correct errors in a received message, equation 1 needs to be solved. The following notations will be used from now on. Let $X = (x_1 \dots x_r)$ be the syndrome vector $\vec{s}$, $Z = (z_t \dots z_1)$ be the vector which each entries z_l denotes the error location α^{k_l} or zero since there is a possibility that only $\mu \le t$ errors occur (μ is the exact weight of error vectors $\vec{e}$), and $Y = (y_1 \dots y_t)$ be the vector which each entries denotes the error values corresponding to the error locations.

By using X, Y, and Z, equation 1 could be rewritten as

$$f_j : \sum_{l=1}^{t} y_l z_l^{i_j} - x_j = 0, \ 1 \le j \le r \tag{2}$$

In this case, the range of all possible solution is very huge. But from the definitions of errors and syndromes, several equations can be added to restrict the range of the solutions. Chen, Reed, Helleseth, and Truong add following equations to restrict equation 2.

$$\sigma_j : \quad x_j^{q^m} - x_j = 0, \qquad 1 \le j \le r \text{ since } x_j \in \mathbb{F}_{q^m}, \tag{3}$$

$$\eta_i : \quad z_i^{n+1} - z_i = 0, \qquad 1 \le i \le t \text{ since } (\alpha^{i_j})^{k_l} \text{are either } n\text{th roots of unity or zero}, \tag{4}$$

$$\lambda_i : \quad y_i^{q-1} - 1 = 0, \qquad 1 \le i \le t \text{ since } a_l \in \mathbb{F}_q \setminus \{0\}. \tag{5}$$

Equations 2, 3, 4, and 5 are collected in system $F = \{f_j, \sigma_j, \eta_i, \lambda_i \mid 1 \le j \le r, \ 1 \le i \le t\}$. The variety defined by F is then called as CRHT syndrome variety.

The Gröbner bases that is obtained by computing F with respect to a lexicographic ordering probably contains a general error locator polynomial $L(z) = \prod_{l=1}^{\mu}(z - \alpha^{k_l})$ of any BCH codes. This research is focused on building system related to F in order to compute the general error locator polynomial of BCH codes.

2 Orsini-Sala's system

The locations and values of errors in a message can be computed using CRHT syndrome variety. However, the system does not guarantee that every error location is distinct. Therefore, Orsini and Sala add other equation to fix this problem. The equation is of the form,

$$\chi_{l,\tilde{l}} : z_l z_{\tilde{l}} \mathrm{p}(n, z_l, z_{\tilde{l}}) = 0, \ 1 \le l < \tilde{l} \le t \tag{6}$$

Equation 6, together with equations in F then generate the ideal

$$I = \left\langle f_j, \sigma_j, \eta_i, \lambda_i, \chi_{l,\tilde{l}} \;\middle|\; 1 \le j \le r, \ 1 \le i \le t, \ 1 \le l < \tilde{l} \le t \right\rangle$$

which is used to compute the Gröbner bases to find the general error locator polynomial. Suppose that G_I is the reduced Gröbner bases of ideal I with respect to lexicographic ordering, then the polynomial $L_z(X, z_t) \in G_I$ is the general error locator polynomial of code C and is obtained by using Orsini-Sala's system I.

The following algorithm is developed by Orsini and Sala to compute error locations by substituting syndrome $\vec{s}$ to general error locator polynomial $L_z(X, z_t) \in G_I$ and is used to decode messages in the later system.

Algorithm 1 Orsini-Sala decoding algorithm

```
Input: $\vec{s} = (s_1 \dots s_r)$ and $L_z(X, z_t) = \sum_{i=0}^{t-1} a_i(X) z_t^i + z_t^t \in G$
  $\mu \leftarrow t$
  while $a_{t-\mu}(\vec{s}) = 0$ do
      $\mu \leftarrow \mu - 1$
  end while
Output: $\mu$ and $L_z(\vec{s}, z_t)/(z_t^{t-\mu})$
```

Note that the algorithm above is used to decode a code after it's general error locator polynomial is found. The general error locator polynomial is computed in the preprocessing of Orsini-Sala's method and is the main object in this research.

3 Fushisato's system

General error locator polynomial of any BCH code C can be computed using Orsini-Sala's system I. However, the complexity of the computation of the Gröbner bases of any system depends on the degrees of polynomials in the system. Thus, it follows that the computation time of the Gröbner bases of Orsini-Sala's system increases exponentially due to σ_j.

Modifying σ_j in Orsini-Sala's system becomes the main problem in order to reduce the amount of computation time since σ_j has the greatest degree among polynomials in the system. It is known that polynomials having syndromes of type $0, \alpha^i, \alpha^i + \alpha^j \in \mathbb{F}_{q^m}$ are sufficient to correct errors in 2-error-correcting codes. To build polynomial with lower degree than σ_j, Fushisato proposes to utilize the minimal polynomials $m_\alpha(x)$ of every syndromes $0, \alpha^i, \alpha^i + \alpha^j \in \mathbb{F}_{q^m}$. That is to take least common multiple of all minimal polynomials of $0, \alpha^i, \alpha^i + \alpha^j \in \mathbb{F}_{q^m}$. Denote the polynomial by τ_j, then it can be written as

$$\tau_j : \operatorname{lcm}\left\{ m_\alpha(x_j) \;\middle|\; \alpha \in \left\{0, \alpha^{i_1}, \alpha^{i_1} + \alpha^{i_2}\right\} \subseteq \mathbb{F}_{q^m} \right\} = 0$$

Denote Fushisato's system formed by changing σ_j to τ_j by

$$J = \left\langle f_j, \tau_j, \eta_i, \lambda_i, \chi_{l,\tilde{l}} \;\middle|\; 1 \le j \le r, 1 \le i \le t, 1 \le l < \tilde{l} \le t \right\rangle.$$

Theorem 3.1. *The reduced Gröbner bases G_J of J with respect to a lexicographical ordering includes a general error locator polynomial for a 2-error-correcting BCH code C.*

Proof. By using theorem 6.8 in [4], simply take $L_z = g_{221}(X, z) \in G_J$ as the general error locator polynomial where $g_{221}(X, z)$ is a polynomial in G_J with leading term $Lt(g_{221}) = z_2^2$ and leading coefficient $Lc(g_{221}) = 1$ since it satisfies the definition of general error locator polynomial.

Note that Fushisato's system only works on 2-error-correcting codes.

4 t-error syndrome system

Recall the definition of errors and syndromes. Here is a solution set Sol considered as a set containing syndromes associated to errors. Based on the definition, the following statements must be satisfied.

1. If there are no errors, then $0 \in \mathbb{F}_{q^m}$ must be in Sol.
2. If there is 1 error occurs, then Sol must contain syndromes of type $\alpha^{i_1} \in \mathbb{F}_{q^m}$.
3. If there are 2 error occur, then Sol must contain syndromes of type $\alpha^{i_1} + \alpha^{i_2} \in \mathbb{F}_{q^m}$.
4. If there are 3 error occur, then Sol must contain syndromes of type $\alpha^{i_1} + \alpha^{i_2} + \alpha^{i_3} \in \mathbb{F}_{q^m}$.
5. If there are l error occur, then Sol must contain syndromes of type $\displaystyle\sum_{j=1}^{l} \alpha^{i_j} \in \mathbb{F}_{q^m}$.

Since t-error-correcting code means that it can correct up to t errors, it can be concluded that for any t-error-correcting code, the set of all possible syndromes Sol can be written as

$$Sol = \{0\} \bigcup_{l=1}^{t} \left\{ \sum_{j=1}^{l} \alpha^{i_j} \;\middle|\; 0 \leq i_1 < i_2 < \cdots < i_l \leq n-1 \right\} \subseteq \mathbb{F}_{q^m}$$

Definition 4.1. Let $m_\alpha(x)$ be the minimal polynomial of a primitive nth root of unity α. For any t-error-correcting BCH code C, the polynomial with minimum degree containing all possible syndromes for the code in Sol is defined by

$$\Omega_j : \mathrm{lcm}\{m_\alpha(x_j) \;\mid\; \alpha \in Sol \subseteq \mathbb{F}_{q^m}\} = 0$$

The polynomial Ω_j defined in definition 4.1 can be written in simpler form

$$\Omega_j : \prod_{\alpha \in Sol} (x - \alpha) = 0$$

so that it will be easier to compute.

Definition 4.2. The modified system of t-error-correcting codes formed by changing $\sigma_j \in I$ to Ω_j is called t-error syndrome ideal and defined by

$$K = \left\langle f_j, \Omega_j, \eta_i, \lambda_i, \chi_{l,\tilde{l}} \;\middle|\; 1 \leq j \leq r,\ 1 \leq i \leq t,\ 1 \leq l < \tilde{l} \leq t \right\rangle.$$

Theorem 4.3. *The reduced Gröbner bases G_K of K with respect to a lexicographical ordering includes a general error locator polynomial for a t-error-correcting BCH code C.*

Proof. By using theorem 6.8 in [4], simply take $L_z = g_{tt1}(X, z) \in G_K$ as the general error locator polynomial where $g_{tt1}(X, z)$ is a polynomial in G_K with leading term $Lt(g_{tt1}) = z_t^t$ and leading coefficient $Lc(g_{tt1}) = 1$ since it satisfies the definition of general error locator polynomial.

5 Computation results

Below are the results computed for some 3-error-correcting BCH codes using computer algebraic system Risa/Asir.

1. $n = 19, m = 18, S_C = \{1\}$,
   - Orsini-Sala's system I:
     - $\sigma_j : x_j^{262144} - x_j = 0$,
     - GB computation time: 26.1458 seconds,
   - Modified system K:
     - $\Omega_j : x_j^{1160} + x_j^{1122} + x_j^{1008} + x_j^{970} + x_j^{856} + x_j^{818} + x_j^{780} + x_j^{742} + x_j^{704} + x_j^{666} + x_j^{628} + x_j^{590} + x_j^{552} + x_j^{514} + x_j^{476} + x_j^{457} + x_j^{438} + x_j^{419} + x_j^{324} + x_j^{305} + x_j^{286} + x_j^{248} + x_j^{229} + x_j^{172} + x_j^{153} + x_j^{39} + x_j^{20} + x_j = 0$,
     - GB computation time: 1.18 seconds,
   - general error locator polynomial : $L_z = z_3^3 + x_1 z_3^2 + (x_1^{1142} + x_1^{1104} + x_1^{1066} + x_1^{1009} + x_1^{990} + x_1^{952} + x_1^{933} + x_1^{914} + x_1^{876} + x_1^{857} + x_1^{800} + x_1^{781} + x_1^{724} + x_1^{705} + x_1^{648} + x_1^{629} + x_1^{572} + x_1^{553} + x_1^{496} + x_1^{477} + x_1^{439} + x_1^{420} + x_1^{382} + x_1^{363} + x_1^{325} + x_1^{287} + x_1^{268} + x_1^{230} + x_1^{192} + x_1^{154} + x_1^{116} + x_1^{2})z_3 + x_1^{1143} + x_1^{1105} + x_1^{1067} + x_1^{991} + x_1^{953} + x_1^{915} + x_1^{877} + x_1^{820} + x_1^{801} + x_1^{744} + x_1^{725} + x_1^{668} + x_1^{649} + x_1^{592} + x_1^{573} + x_1^{516} + x_1^{497} + x_1^{421} + x_1^{402} + x_1^{383} + x_1^{307} + x_1^{288} + x_1^{269} + x_1^{212} + x_1^{117} + x_1^{98} + x_1^{79} + x_1^{60}$.

2. $n = 37, m = 36, S_C = \{1\}$,
   - Orsini-Sala's system I:
     - $\deg(\sigma_j) = 68719476736$,
     - GB computation time: almost impossible to compute the Gröbner bases of this system,
   - Modified system K:
     - $\deg(\Omega_j) = 8474$,
     - GB computation time: 216.644 seconds,
   - general error locator polynomial : $L_z = z_3^3 + x_1 z_3^2 + (x_1^{8438} + x_1^{8401} + x_1^{8364} + x_1^{8253} + x_1^{8216} + x_1^{8179} + x_1^{8068} + x_1^{8031} + x_1^{7994} + x_1^{7920} + x_1^{7883} + x_1^{7735} + x_1^{7698} + x_1^{7661} + x_1^{7550} + x_1^{7365} + x_1^{7291} + x_1^{7069} + x_1^{7032} + x_1^{6995} + x_1^{6958} + x_1^{6847} + x_1^{6810} + x_1^{6736} + x_1^{6551} + x_1^{6440} + x_1^{6403} + x_1^{6366} + x_1^{6255} + x_1^{6181} + x_1^{6107} + x_1^{6070} + x_1^{6033} + x_1^{5996} + x_1^{5922} + x_1^{5848} + x_1^{5774} + x_1^{5700} + x_1^{5552} + x_1^{5478} + x_1^{5441} + x_1^{5404} + x_1^{5367} + x_1^{5293} + x_1^{5145} + x_1^{5108} + x_1^{5071} + x_1^{4923} + x_1^{4849} + x_1^{4738} + x_1^{4701} + x_1^{4627} + x_1^{4590} + x_1^{4516} + x_1^{4479} + x_1^{4368} + x_1^{4257} + x_1^{4146} + x_1^{4109} + x_1^{4035} + x_1^{3998} + x_1^{3961} + x_1^{3924} + x_1^{3887} + x_1^{3850} + x_1^{3813} + x_1^{3702} + x_1^{3628} + x_1^{3591} + x_1^{3443} + x_1^{3406} + x_1^{3295} + x_1^{3258} + x_1^{3073} + x_1^{3036} + x_1^{2962} + x_1^{2925} + x_1^{2888} + x_1^{2851} + x_1^{2814} + x_1^{2740} + x_1^{2703} + x_1^{2555} + x_1^{2370} + x_1^{2296} + x_1^{2185} + x_1^{2111} + x_1^{2074} + x_1^{2037} + x_1^{2000} + x_1^{1963} + x_1^{1889} + x_1^{1815} + x_1^{1556} + x_1^{1445} + x_1^{1408} + x_1^{1371} + x_1^{1297} + x_1^{1260} + x_1^{1223} + x_1^{1112} + x_1^{1038} + x_1^{964} + x_1^{927} + x_1^{890} + x_1^{742} + x_1^{668} + x_1^{631} + x_1^{557} + x_1^{520} + x_1^{298} + x_1^{261} + x_1^{224} + x_1^{187} + x_1^{76} + x_1^{2})z_3 + x_1^{8439} + x_1^{8365} + x_1^{8069} + x_1^{7995} + x_1^{7958} + x_1^{7884} + x_1^{7847} + x_1^{7773} + x_1^{7736} + x_1^{7514} + x_1^{7477} + x_1^{7329} + x_1^{7255} + x_1^{7181} + x_1^{7144} + x_1^{7107} + x_1^{7070} + x_1^{7033} + x_1^{6996} + x_1^{6885} + x_1^{6848} + x_1^{6663} + x_1^{6515} + x_1^{6478} + x_1^{6441} + x_1^{6404} + x_1^{6330} + x_1^{6145} + x_1^{6108} + x_1^{6034} + x_1^{5923} + x_1^{5886} + x_1^{5590} + x_1^{5553} + x_1^{5479} + x_1^{5331} +$

$$x_1^{5257}+x_1^{5220}+x_1^{4998}+x_1^{4961}+x_1^{4924}+x_1^{4887}+x_1^{4850}+x_1^{4776}+x_1^{4702}+x_1^{4665}+x_1^{4628}+x_1^{4443}+ x_1^{4406}+x_1^{4369}+x_1^{4332}+x_1^{4295}+x_1^{4258}+x_1^{4221}+x_1^{4184}+x_1^{4110}+x_1^{4073}+x_1^{3999}+x_1^{3740}+x_1^{3703}+ x_1^{3666}+x_1^{3629}+x_1^{3370}+x_1^{3333}+x_1^{3296}+x_1^{3148}+x_1^{3074}+x_1^{3037}+x_1^{3000}+x_1^{2926}+x_1^{2889}+x_1^{2815}+ x_1^{2630}+x_1^{2593}+x_1^{2556}+x_1^{2519}+x_1^{2408}+x_1^{2260}+x_1^{2223}+x_1^{2149}+x_1^{2075}+x_1^{2001}+x_1^{1964}+x_1^{1890}+ x_1^{1853}+x_1^{1742}+x_1^{1705}+x_1^{1668}+x_1^{1594}+x_1^{1520}+x_1^{1483}+x_1^{1446}+x_1^{1335}+x_1^{1298}+x_1^{1187}+x_1^{1113}+ x_1^{1002}+x_1^{891}+x_1^{854}+x_1^{817}+x_1^{743}+x_1^{669}+x_1^{484}+x_1^{373}+x_1^{336}+x_1^{299}+x_1^{262}+x_1^{188}+x_1^{77}+x_1^{40}.$$

3. $n = 61, m = 60, S_C = \{1\}$,
    - Orsini-Sala's system I:
        - $\deg(\sigma_j) = 1152921504606846976$,
        - GB computation time: almost impossible to compute the Gröbner bases of this system,
    - Modified system K:
        - $\deg(\Omega_j) = 37882$,
        - GB computation time: 1564.78 seconds,
    - The general error locator polynomial is a huge polynomial.

6 Summary

The system K is sufficient to obtain the general error locator polynomial of t-error-correcting BCH codes since $\Omega_j \in K$ contain all possible syndromes for the codes. In this paper, the general error locator polynomial of 3-error-correcting BCH codes can be obtained and the amount of computation time of the lexicographic Gröbner bases is greatly reduced.

Acknowledgment

The researchers would like to thank Japan student service organization (JASSO) for the financial support in the research, to all previous researchers in these topics, and to the developer of strong computer algebraic system Risa/Asir. Also thank to researchers's family, DDP KU-ITB 2013's students, computational science of ITB and Kanazawa University's lecturers, all Indonesian people in Ishikawa, Pudy Kusumaningrum, and Kanazawa University for all the support.

References

[1] Fushisato, T., A BCH decoding algorithm using the Gröbner bases of a polynomial ideal. Master's thesis, Kanazawa University, January 2014. (in Japanese)

[2] Fushisato, T., Ohara, K., Effective computation of general error locator polynomials of binary BCH codes with $t = 2$, in preparation.

[3] Miyake, S., On decoding algorithm for cyclic codes using Gröbner bases. Master's thesis, Kobe University, February 2012. (in Japanese)

[4] Orsini, E., Sala, M., Correcting errors and erasures via the syndrome variety. Journal of Pure and Applied Algebra **200** (2005), 191-226.